ISO 27001:2013 VE ISO 27001:2005 ARASINDAKİ TEMEL FARKLAR NELERDİR?

Bilgi Güvenliği Yönetim Sistemi (BGYS-(in Eng. ISMS)'nin uluslararası standardı 2005 yılında ISO 27001:2005 olarak yayımlanmıştı. 2006 yılında ise Türk Standartları Enstitüsü tarafından Türkçe'ye çevrilmiş ve TS ISO/IEC 27001 olarak yayımlanmıştı.

ISO 27001:2013 standardı 25.09.2013 tarihinde yeni sürüm olarak yayınlandı.

ISO 27001:2013 ile ISO 27001:2005 Arasındaki temel farklar nelerdir?.

Yapıya Genel Bir Bakış

ISO 27001:2013, ISO22301:2012 ile gördüğümüz Annex SL ile uyumludur.. Annex SL tüm ISO standartlarına genel bir çerçeve yapısı oluşturuyor. Tüm yönetim sistemlerinde bulunması gereken temel bileşenlerin yanı sıra standarda özel başlıkların konulmasına olanak sağlayan bu çatı yapısı, birden fazla yönetim sistemine sahip kuruluşlar için hem yönetim anlamında hem de bu yönetim sistemlerinin denetimi anlamında kolaylık sağlayacaktır. Bu yapı ile tüm standartlarda bulunacak temel başlıklar aşağıdaki gibi olacaktır;

0 Introduction /Giriş
1 Scope /Kapsam
2 Normative references / Atıf yapılan standartlar ve/veya dokümanlar
3 Terms and definitions /Terimler ve tarifleri
4 Context of the organization / Kurum Bağlamı
5 Leadership /Liderlik
6 Planning /Planlama
7 Support /Destek
8 Operation /Operasyon
9 Performance evaluation /Performans değerlendirme
10 Improvement /İyileştirme
Ek olarak sadece 'EK-A' bulunduğu bununla birlikte eski standartta yer alan EK-B ve EK-C olmadığını görüyoruz. Tüm kontroller EK-A' da yer almaktadır.

İlgili Taraflar

Yeni 27001 standardı BGYS ana girdileri tanımlamada önemli bir yer tutacak olan ilgili taraflarla alakalı olarak '4.2 ' Maddesinde;

Tüm ilgili tarafların tanımlanması ve yasal/düzenleyici dâhil tüm gereksinimleri ile tanımlanmasını şart koşuluyor.

Risk Değerlendirme ve İyileştirme

Uzun yıllar en iyi uygulama örneği olarak yerini koruyacak olan; varlık, açıklık, tehdit temelli risk değerlendirme yeni 27001 standardı ile yerini gizlilik, bütünlük ve erişilebilirlik temelli bir risk tanımlamaya bırakmış durumda.

6.1.2 c.1 Maddesi uyarınca;

Firmalar kapsam dahilinde ki bilginin gizlilik, bütünlük ve erişebilirliğinin kaybı durumunda oluşacak riski belirlemek üzere bilgi güvenliği risk değerlendirme sürecini uygulamalıdır.

Risk seviyesini belirlemek için olasılık ve etki bileşenleri ise yerini koruyor.

Yeni sürümde "risk sahibi" kavramı yer almaktadır. Risklere bir sahip atanacak ve risk sahipleri risk işleme planının ve artık risklerin onaylanmasından sorumlu kişiler olarak standartta tanımlanmaktadır.

Not: Yeni standart risk işleme yönetiminin dokümante edilmesini şart koşmuyor. Bununla birlikte risk işleme sürecinin tanımlanması gerekiyor.

Düzeltici ve Önleyici Faaliyetler

İlk fazda önleyici faaliyetlerin olmadığını söylemek yanlış olmaz. Önleyici faaliyetler risk işleme ve iyileştirme adımlarına dağıtılmış durumda.

Düzeltici faaliyetler için ise, eski standarda kafa karışıklığına sebebiyet veren durum ortadan kaldırılmış olduğu görülüyor. Düzeltici faaliyetlerin bir uygunsuzluğa verilen ilk tepki ve bir uygunsuzluğun kök nedenlerini ortadan kaldırmak üzere ikiye ayrıldığını görüyoruz.

İletişim

Bilgi güvenliğinin sağlanması için gereken iletişim ile ilgili olarak yeni bir madde eklenmiştir.

(Madde 7.4)

Bu madde uyarınca;

Kiminle, ne zaman, kim ve hakkında iletişime geçileceğinin tanımlanması sağlanıyor.

Dokümante Edilmiş Bilgi

Yeni standart ‘belgeler’ ve ‘kayıtlar’ kavramını birleştirerek ‘dokümante edilmiş bilgi’ kavramını getiriyor. Doküman kontrolü ile ilgili kuralların eski standarda göre değişmediği ve ‘belgeler’ ve ‘kayıtlar’ ın her ikisi içinde geçerli olacağı öngörülüyor.

4.3.1 Maddesinin kaldırıldığı ve gerek duyulan merkezi bir doküman listesinin olmadığını görüyoruz.

Eski standartta yer alan doküman yönetimi, düzeltici faaliyet v.b zorunlu olarak olması gereken belgelerin olmadığı bununla birlikte bu süreçlerin yönetilmesi ve işletilmesi ile ilgili kayıtların tutulması zorunluluğu bulunuyor. Daha farklı ifadelerle düzeltici faaliyet dokümanı yazılı olarak olmasa bile bu sürecin işletilmesi ile ilgili kayıtların tutulması zorunlu.

Hedefler, İzleme ve Ölçme

Yeni standartta hedeflerin net olarak tanımlanması ve 9.1 maddesi uyarınca, ölçmenin kim tarafından ne zaman yapılacağı, sonuçları kimin analiz edip değerlendirileceği belirtilmeli ve ek olarak kapsamlı planların hedeflere nasıl ulaşılacağı açıklayacak şekilde olması gerekiyor.

ISO 27001 Bilgi Güvenliği Hizmetleri: http://www.btyon.com.tr/bilgi_guvenligi.php

ISO 27001 Bilgi Güvenliği Eğitimleri: http://www.btyon.com.tr/bilgi_guvenligi_egitimleri.php